Overview of Web Services Security

Technologies and Markets

Jason Bloomberg
ZapThink LLC

zapthink

The risks inherent in emerging technologies

- Web Services represent a new set of approaches to distributed computing, based on open standards.
- Standards are always changing, and so are the technologies.
- How should companies reduce the risks of Web Services?

Security is critical to Web Services

Security is the primary roadblock for Web Services adoption

- Pent up demand in the enterprise for B2B applications of Web Services
- Many new vendors and products coming to market
- Established IT security vendors Web Service-enabling their products

Identity Management is Often the Overriding Issue

- Too many passwords for too many systems
- Problems administering users
  - Password change requests eating up resources
  - Difficulty removing users from the system
- Too many people with root access
- Unknown security holes
- No enterprise ID policy

The “20 doors” problem

If your company has 20 doors, and you lock 19, then you are not secure

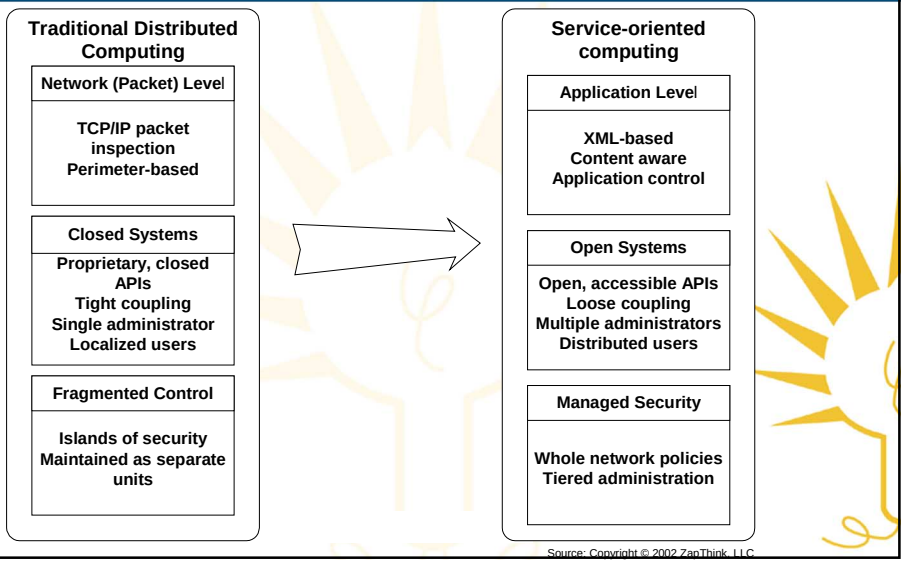
- Any Web Services security approach must be a part of a comprehensive enterprise security initiative
- Web Services can help secure the enterprise, and the enterprise must secure their Web Services

The “200 doors” problem

If your company has 200 doors, and you lock 199, then you are not secure

- Security exhibits diseconomies of scale

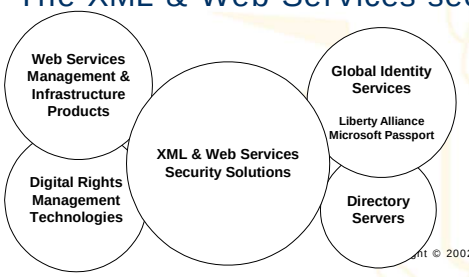
Security in an SOA



Context for Web Services security

- The overall IT security market

- The XML & Web Services security market



Both
Perimeter network security
and
application-level security

A look at the fundamentals…

A quick overview of application security technology

Principles of application security

- Authentication
  - Are you who you say you are?
- Authorization
  - Are you authorized to send the message?
- Confidentiality
  - Is the message safe from prying eyes?
- Data integrity
  - Can you guarantee the message hasn't been tampered with?
- Non-repudiation
  - Can you confirm the sender sent the message and the recipient received it?

IT security fundamentals

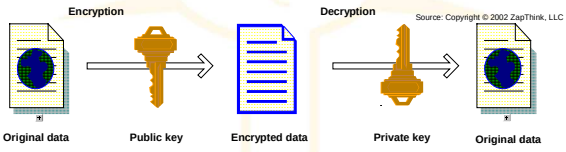
- Basic HTTP security
  - Passwords not secure
  - Limited use
- SSL (Secure Sockets Layer)
  - Point-to-point
  - Designed for browsers and Web servers

IT security fundamentals (cont.)

Encryption & decryption

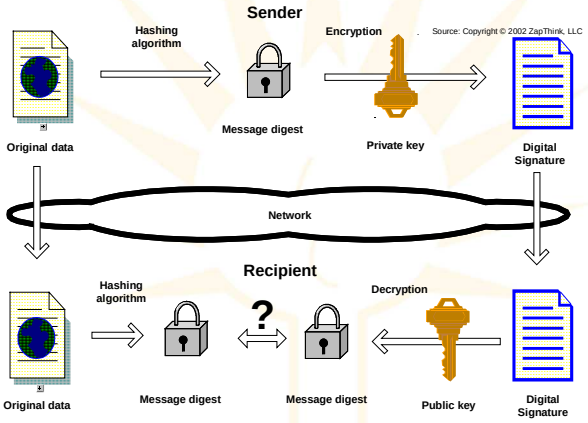
- Symmetric key approaches

- Asymmetric key approaches



IT security fundamentals (cont.)

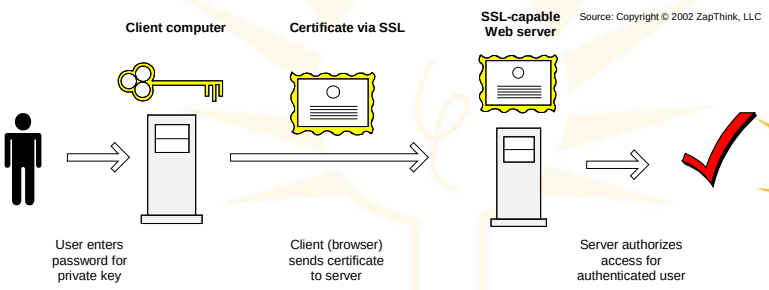
Digital signatures



IT security fundamentals (cont.)

Digital certificates

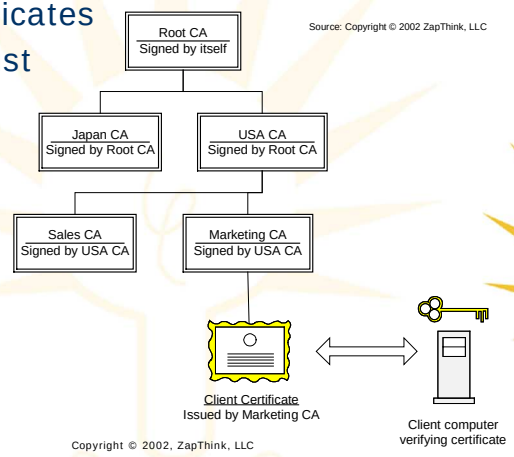
- Authorization with certificates



IT security fundamentals (cont.)

Public Key Infrastructure (PKI)

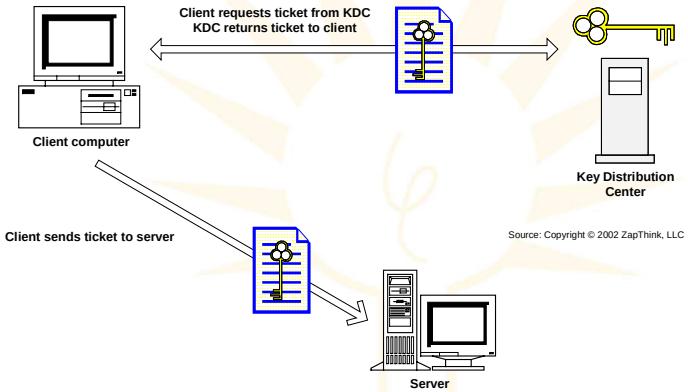
- Managing certificates
- Establishing trust



Source: Copyright © 2002 ZapThink, LLC

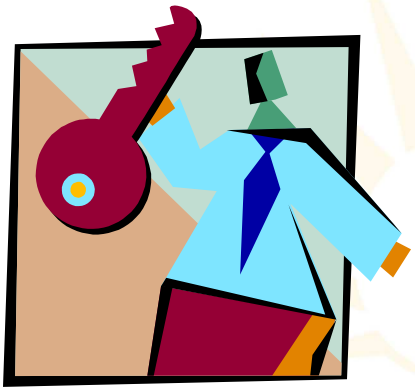
IT security fundamentals (cont.)

Kerberos



Source: Copyright © 2002 ZapThink, LLC

XML & Web Services security technologies

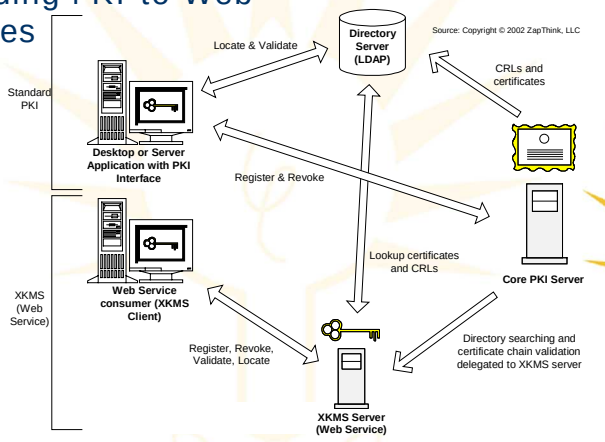


- XML Digital Signatures
- XML Encryption
- XACML (XML Access Control Markup Language)

XML & Web Services security technologies (cont.)

XKMS (XML Key Management Services)

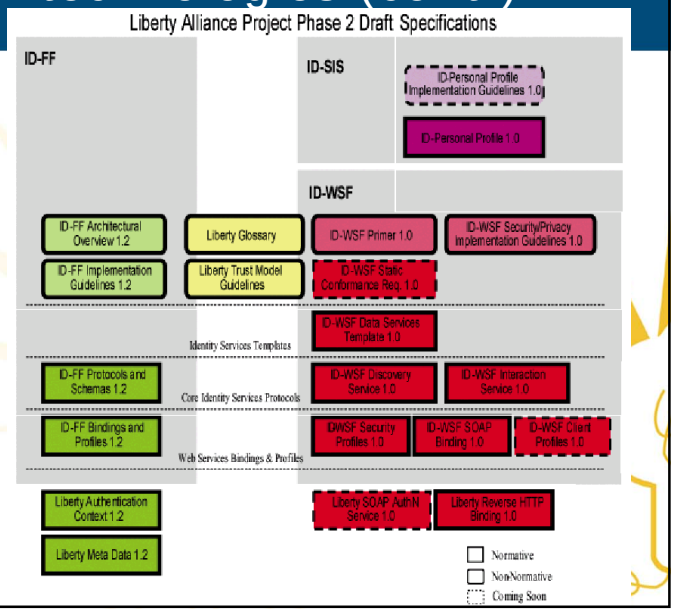
- Extending PKI to Web Services



XML & Web Services security technologies (cont.)

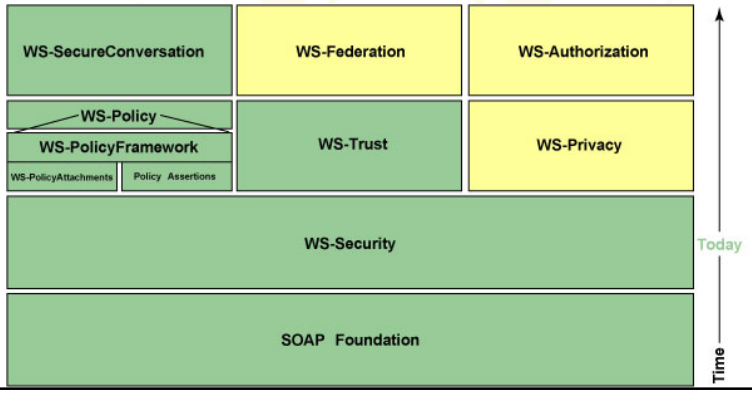
- SAML (Security Assertion Markup Language)
  - A standard for exchanging authentication and authorization information (known as *assertions*) between security domains
- ID-FF (Liberty Identity Federation Framework)
  - Multiparty B2B federated identity specification proposed by the Liberty Alliance consortium

XML & Web Services security technologies (cont.)



XML & Web Services security technologies (cont.)

- WS-Security
  - The first of a broad set of specifications that abstract a broad range of existing security frameworks and technologies, including both PKI and Kerberos.



XML & Web Services security technologies (cont.)

- WS-Policy
  - Accommodates the expression of domain specific policy languages in a way that leverages different domain knowledge within a consistent Web Services Framework.
- WS-Trust
  - Defines a set of interfaces that a secure token service may provide for the issuance, exchange, and validation of security tokens.
- WS-SecureConversation
  - Describes how security tokens can be used within the context of policy-defined trust relationships to allow multiple service requesters and service providers to securely exchange information over the duration of a conversation.

What are vendors doing?

Market segmentation

Private Web Services Network Providers
Bang Networks
Flamenco Networks
Grand Central
Slam Dunk Networks

Access & Policy Mgmt Vendors
Waveset

Enterprise Security Services
TruSecure, IBM
EDS, ISS, CA

Web Services Infrastructure Management Vendors
Systinet, AmberPoint
Cape Clear, Iona
Bowstreet, Flamenco

Web Services Security Platforms
Westbridge Technology
Quadrasis, Primordial
Entrust, Actional
Baltimore Technologies

Global Trust Services
Verisign
Entrust
beTRUSTed

PKI Vendors
RSA Security
VeriSign
Baltimore Technologies
Entrust, CA

Secure Integration/EAI Vendors
webMethods
Vitria, SeeBeyond
Tibco, IBM
Actional, BEA

Software XML Firewalls
Reactivity
Quadrasis
Westbridge Technology
Vordel

Identity/Single Sign-on Vendors
Netegrity, Oblix
Open Network
Entegrity, Entrust
OneName, CA
Novell, RSA Security

Web Services Security Toolkit Vendors
RSA Security
IBM, Systinet, Entrust
Netegrity, nCipher
Phaos Technology

Security Service Providers
McAfee
Symantec

Source: Copyright © 2002 ZapThink, LLC

Approaches to the market

- Focused technology startups
  - Survivors have funding, solid management & engineering teams
- "Established" Web Services vendors
  - Have small but significant customer base
- Established security software companies
  - Customers, technology depth, financial resources

Fundamental security principles

- There is no such thing as perfect security
  - Perfectly secure networks and systems are an impossibility
- It is impossible to list of all the risks facing a company
  - There is always the possibility of an entirely unexpected risk
- Security is never complete
  - Security is an ongoing, ever-changing process
- There is no way to accurately calculate the risks that security addresses
  - Any security failure may lead to unexpected consequences
- Security exhibits diseconomies of scale
  - How much security is enough is a subjective call for business management (not IT)

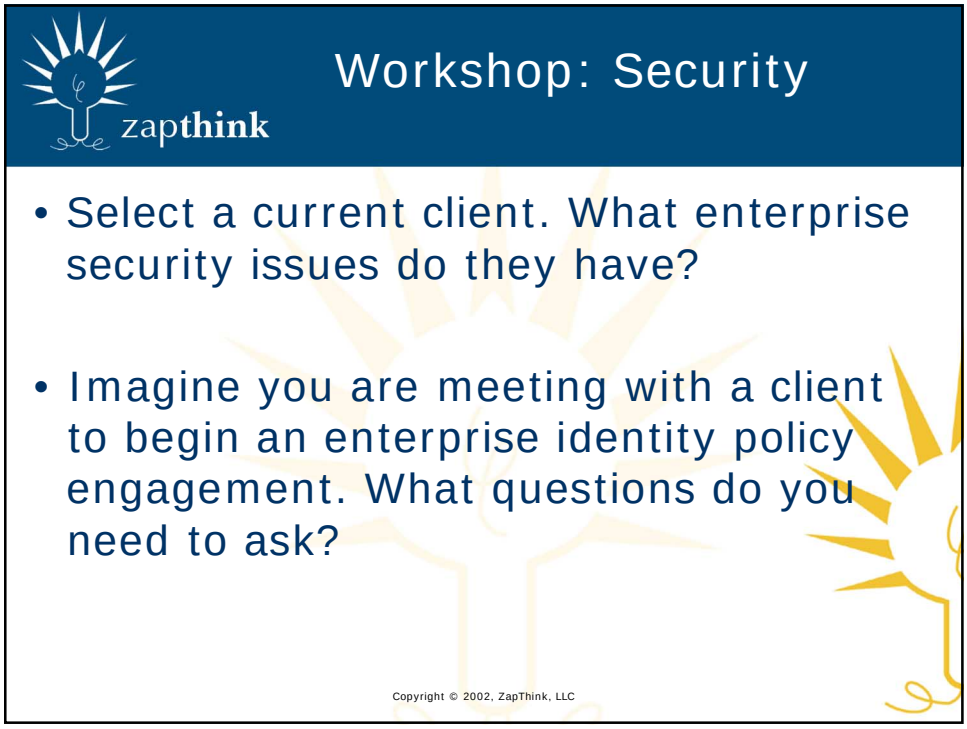
Importance for Samsung SDS

zapthink

- Security engagements may precede SOA engagements
- Identity management issues must be resolved before a company can build a broad-based SOA
- Using Web Services to address enterprise security more applicable than securing Web Services for many companies

zapthink

Questions & Discussion


zapthink
Workshop: Security
• Select a current client. What enterprise security issues do they have?
• Imagine you are meeting with a client to begin an enterprise identity policy engagement. What questions do you need to ask?
Copyright © 2002, ZapThink, LLC